изображениях, подаваемых на видеокамеру, свидетельствует о наличии взаимосвязи между обрабатываемой информацией и ПЭМИ. Следовательно, побочное электромагнитное излучение от сканера штрих-кодов является информативным и теоретически из него можно извлечь информативную составляющую.

Поставленная перед нами задача решена, но необходимы дальнейшие исследования для выделения информативного сигнала и практического подтверждения теоретических результатов.

**Список литературы**

1. *Сребнев В. И.* Поисковый радиомониторинг: проблемы, методики, аппаратура // Системы безопасности. 1999. 24. Январь-февраль. С. 58–63.

2. *Van Eck W*. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? // Computers & Security : journal. Elsevier Advanced Technology Publications, 1985. Vol. 4, Is. 4. P. 269–286. ISSN01674048. DOI: 10.1016/0167–4048(85)90046-X.

3. *Markus G*. Kuhn Security Limits for Compromising Emanations // Cryptographic Hardware and Embedded Systems. 2005. Vol. 3659. P. 265–279. DOI: 10.1007/11545262_20.

4. *Vuagnoux M*., *Pasini S.* Compromising electromagnetic emanations of wired and wireless keyboards // Proceeding SSYM'09 Proceedings of the 18th conference on USENIX security symposium. 2009. P. 1–16

5. juhztfzujb. Compromising electromagnetic emanations of wired keyboards 2 [Любительское видео] // YouTube. 23 октября 2008. https://youtu.be/d926EztWimM (дата обращения: 15.09.2017).

6. ФЗ № 162-ФЗ «О стандартизации в Российской Федерации» (с изменениями и дополнениями) от 29 июня 2015 г. [Электронный ресурс]. 2015. Режим доступа: http://www.gost.ru/wps/wcm/connect/43debd0048f477a5a38dfb-56779c92ad/FZ_29.06.2015_162.pdf? MOD=AJPERES

УДК 004

**М. Н. Вольхина, К. Л. Стойчин**
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

## ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСУ ТП

*Аннотация.* В настоящее время автоматизированные системы управления технологическими процессами (далее — АСУ ТП) имеют широкое распространение в промышленной и производственной сфере. Применение АСУ ТП охваты-

вает множество задач, решаемых как для оборонно-промышленного комплекса, так и для предприятий малого бизнеса. Нарушения технологического процесса, вызванные инцидентом информационной безопасности, могут повлечь за собой ущерб как для Российской Федерации в целом, так и для репутации производителя. Например, использование АСУ ТП для изготовления снаряда высокоточного оружия при положительно свершившемся инциденте информационной безопасности может оказать влияние на вооруженные силы. При том же исходе в малом бизнесе, например при производстве авторучек, последствия инцидента информационной безопасности могут нанести вред репутации и, несомненно, материальной составляющей производителя.

Исходя из вышеизложенного, следует, что актуальность защиты информационных процессов, протекающих в АСУ ТП, сегодня является крайней высокой проблемой, так как угрозы, исходящие от злоумышленников, постоянно усовершенствуются.

*Ключевые слова:* автоматизация; АСУ ТП; уровни; угрозы; уязвимости; безопасность.

**Общие сведения об АСУ ТП**

Автоматизированная система управления технологическим процессом — это человеко-машинная система управления, обеспечивающая автоматизированный сбор и обработку информации, необходимой для оптимизации управления технологическим объектом в соответствии с принятым критерием.

Стоит отметить, что участие оператора сведено к минимуму, но все же присутствует на уровне реализации и принятия наиболее ответственных решений [1].

Главными целями автоматизации технологического процесса являются:

- централизованный контроль управления технологическим оборудованием;
- сбор и первичная обработка данных о процессе для обеспечения персонала актуальной информацией;
- повышение безопасности и надежности функционирования объекта;
- уменьшение влияния человеческого фактора на управляемый процесс.

Таким образом, главной целью АСУ ТП является обеспечение оптимального функционирования технологического процесса.

Как правило, АСУ ТП состоит из трех уровней, которые представляют собой единую систему операторского управления технологическим процессом в виде одного или нескольких пультов управления, средства обработки информации о ходе процесса и типовые элементы автоматики (датчики, устройства управления и исполнительные устройства) [2].

Предлагаю рассмотреть подробнее каждый уровень. Самый нижний, первый уровень — датчики и исполнительные механизмы, передают данные от устройств по линиям связи на средний уровень. Далее идет средний уровень, который включает в себя программируемые логические контроллеры и операторские панели. Контроллеры и панели получают данные с нижнего уровня и передают на верхний уровень для принятия решения по управлению объектом или процессом. Завершает процесс верхний уровень — это операторские автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением, телекоммуникационное оборудование (маршрутизаторы, коммутаторы), а также каналы связи. На автоматизированных рабочих местах выводится состояние технологического процесса, и отсюда при необходимости оператором подаются команды на изменение какого-либо параметра.

**Угрозы АСУ ТП**

Современные АСУ ТП подвержены разнообразным угрозам со стороны внутренних и внешних злоумышленников (террористические, экстремистские и враждебно настроенные группы) с целью вывести систему из строя.

Необходимо отметить, что сами производители и потребители не всегда обеспечивают должную безопасность, при этом не выполняя необходимые требования по безопасности своих систем. Из-за непрерывности технологических процессов базовые компоненты систем управления (индустриальные протоколы, операционные системы, системы управления базами данных) регулярно не обновляются. Все вышесказанное в совокупности приводит к появлению уязвимостей в системе, в результате которых реализуются новые угрозы.

Сегодня для АСУ ТП наиболее актуальны угрозы сбоя, отказов и нарушения режима работы, распространение вредоносного программного обеспечения [3]. Реализация этих угроз непосредственно связана с:

- ошибочными действиями пользователей;
- случайным доступом посторонних лиц к системам;
- несанкционированным подключением USB-устройств к автоматизированным рабочим местам пользователей, а также к сети Интернет.

Решение данной проблемы сводится к комплексу мер, направленных на обеспечение безопасности информации в целом. Стоит отметить, что на производстве необходимо уделять внимание не только обеспечению конфиденциальности данных и информации, но и обеспечению непрерывности и целостности самого технологического процесса. Ведь мало кому будут полезны и интересны данные с датчиков, а если злоумышленнику удастся вывести из строя и остановить производство, это может нанести огромные ущерб предприятию.

Поэтому задача обеспечения безопасности АСУ ТП — это прежде всего обеспечение безопасности технологических процессов. Обезопасить техноло-

гические процессы — это значит оградить их от любых несанкционированных воздействий информационного характера, которые создают возможность некорректного выполнения технологических процессов.

**Список литературы**

1. ГОСТ 34.003–1990 Автоматизированные системы. Термины и определения.

2. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31.

3. Positive Technologies: отчет об уязвимостях АСУ ТП за 2016 год. URL: http://www.safe-surf.ru.

УДК 004.056.53

**И. В. Кротенко**
Научный руководитель: канд. тех. наук, доц. А. С. Лучинин
Уральский федеральный университет, Екатеринбург

## PLC-СИСТЕМЫ КАК СРЕДСТВО ОСУЩЕСТВЛЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

*Аннотация.* Существуют различные области применения систем передачи информации по сети 220 В и множество технических решений на их основе. Примерами могут быть распределенные системы управления и учета в цехах, системах жизнеобеспечения зданий, системах складского хранения, средствах учета потребления электроэнергии, системах охранной и пожарной сигнализации. Существуют возможности реализации концепции «умного дома», в котором вся бытовая электроника объединена в единую информационную сеть с возможностью централизованного управления [1]. Однако структура информационных пакетов, передаваемых такими устройствами по сети, слабо изучена и различна в конкретных случаях у разных производителей таких устройств. Все это потенциально может быть использовано для несанкционированного доступа к информации [2].

*Ключевые слова:* информация; безопасность; передача информации; техническая защита информации; сеть 220 В; PLC; несанкционированный доступ к информации.